



syslog를 관리합니다

SANtricity 11.8

NetApp
December 16, 2024

목차

| | |
|---|---|
| syslog를 관리합니다 | 1 |
| 감사 로그 활동을 봅니다 | 1 |
| 감사 로그 정책을 정의합니다 | 3 |
| 감사 로그에서 이벤트를 삭제합니다 | 4 |
| 감사 로그를 위해 syslog 서버를 구성합니다 | 5 |
| 감사 로그 레코드에 대한 syslog 서버 설정을 편집합니다 | 6 |

syslog를 관리합니다

감사 로그 활동을 봅니다

보안 관리자 권한이 있는 사용자는 감사 로그를 보고 사용자 작업, 인증 실패, 잘못된 로그인 시도 및 사용자 세션 수명을 모니터링할 수 있습니다.

시작하기 전에

보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 감사 로그 탭을 선택합니다.

감사 로그 작업은 다음과 같은 정보 열이 포함된 표 형식으로 표시됩니다.

- * 날짜/시간 * — 스토리지 배열이 이벤트를 감지한 때의 타임스탬프(GMT).
- * 사용자 이름 * — 이벤트와 연결된 사용자 이름입니다. 스토리지 시스템에서 인증되지 않은 작업의 경우 "N/A"가 사용자 이름으로 나타납니다. 인증되지 않은 작업은 내부 프록시 또는 다른 메커니즘에 의해 트리거될 수 있습니다.
- * 상태 코드 * — 작업의 HTTP 상태 코드(200, 400 등) 및 이벤트와 관련된 설명 텍스트입니다.
- * URL 액세스 * — 전체 URL(호스트 포함) 및 쿼리 문자열
- * 클라이언트 IP 주소 * — 이벤트와 연결된 클라이언트의 IP 주소입니다.
- * 소스 * — 이벤트와 연결된 로깅 소스로, System Manager, CLI, 웹 서비스 또는 지원 셸이 될 수 있습니다.
- * 설명 * — 해당되는 경우 이벤트에 대한 추가 정보

3. 감사 로그 페이지의 선택 항목을 사용하여 이벤트를 보고 관리할 수 있습니다.

선택 세부 사항

| 선택 | 설명 |
|--------------|---|
| 이벤트 표시... | 날짜 범위별로 표시되는 이벤트 제한(지난 24시간, 지난 7일, 지난 30일 또는 사용자 지정 날짜 범위) |
| 필터 | 필드에 입력한 문자로 표시되는 이벤트를 제한합니다. 정확히 일치하는 단어를 찾으려면 따옴표("")를 사용하고, 하나 이상의 단어를 반환하려면 을 OR 입력하고, 단어를 생략하려면 대시(--)를 입력합니다. |
| 새로 고침 | 페이지를 최신 이벤트로 업데이트하려면 * Refresh * 를 선택합니다. |
| 설정 보기/편집 | 설정 보기/편집 * 을 선택하여 전체 로그 정책 및 기록할 작업 수준을 지정할 수 있는 대화 상자를 엽니다. |
| 이벤트를 삭제합니다 | 페이지에서 이전 이벤트를 제거할 수 있는 대화 상자를 열려면 * 삭제 * 를 선택합니다. |
| 열 표시/숨기기 | <p>표시/숨기기 * 열 아이콘을  클릭하여 테이블에 표시할 추가 열을 선택합니다. 추가 열은 다음과 같습니다.</p> <ul style="list-style-type: none"> * Method * — HTTP 메서드(예: POST, GET, DELETE 등). * CLI 명령 실행됨 * — Secure CLI 요청에 대해 실행되는 CLI 명령(문법) * CLI return Status * — CLI 상태 코드 또는 클라이언트의 입력 파일 요청입니다. * 기호 프로시저 * — 기호 프로시저가 실행됩니다. * SSH 이벤트 유형 * — 로그인, 로그아웃 및 login_fail과 같은 SSH(Secure Shell) 이벤트 유형 * SSH 세션 PID * — SSH 세션의 프로세스 ID 번호입니다. * SSH 세션 지속 시간 * — 사용자가 로그인한 시간(초)입니다. * 인증 유형 * — 유형에는 로컬 사용자, LDAP, SAML 및 액세스 토큰이 포함될 수 있습니다. * 인증 ID * — 인증된 세션의 ID입니다. |
| 열 필터를 전환합니다 | 각 열의 필터링 필드를 열려면 * 전환 * 아이콘을  클릭합니다. 열 필드에 문자를 입력하여 해당 문자로 표시되는 이벤트를 제한합니다. 필터링 필드를 닫으려면 아이콘을 다시 클릭합니다. |
| 변경 내용을 취소합니다 | 테이블을 기본 구성으로 되돌리려면 * 실행 취소 * 아이콘을  클릭합니다. |
| 내보내기 | 내보내기 * 를 클릭하여 테이블 데이터를 CSV(쉼표로 구분된 값) 파일에 저장합니다. |

감사 로그 정책을 정의합니다

덮어쓰기 정책과 감사 로그에 기록된 이벤트 유형을 변경할 수 있습니다.

시작하기 전에

보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

이 작업에 대해

이 작업에서는 이전 이벤트를 덮어쓰는 정책과 이벤트 유형을 기록하는 정책을 비롯한 감사 로그 설정을 변경하는 방법에 대해 설명합니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. Audit Log(감사 로그) * 탭을 선택합니다.
3. 설정 보기/편집 * 을 선택합니다.

감사 로그 설정 대화 상자가 열립니다.

4. 기록된 이벤트 유형 또는 덮어쓰기 정책을 변경합니다.

| 설정 | 설명 |
|--------------|--|
| 정책 덮어쓰기 | <p>최대 용량에 도달할 때 이전 이벤트를 덮어쓰는 정책을 결정합니다.</p> <ul style="list-style-type: none"> * 감사 로그가 가득 차면 감사 로그의 가장 오래된 이벤트를 덮어쓰도록 허용 * — 감사 로그가 50,000개 레코드에 도달할 때 이전 이벤트를 덮어씁니다. * * 감사 로그 이벤트를 수동으로 삭제해야 함 * — 이벤트가 자동으로 삭제되지 않도록 지정합니다. 대신 설정된 백분율로 임계값 경고가 표시됩니다. 이벤트는 수동으로 삭제해야 합니다. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> 덮어쓰기 정책을 사용하지 않도록 설정하고 감사 로그 항목이 최대 한도에 도달하면 보안 관리자 권한이 없는 사용자는 System Manager에 액세스할 수 없습니다. 보안 관리자 권한이 없는 사용자에게 대한 시스템 액세스를 복원하려면 보안 관리자 역할에 할당된 사용자가 이전 이벤트 레코드를 삭제해야 합니다.</p> <p> 감사 로그 보관을 위해 syslog 서버가 구성된 경우 덮어쓰기 정책은 적용되지 않습니다.</p> </div> |
| 기록할 작업 수준입니다 | <p>기록할 이벤트 유형을 결정합니다.</p> <ul style="list-style-type: none"> * * 수정 이벤트만 기록 * — 사용자 작업이 시스템에서 변경을 수행하는 이벤트만 표시합니다. * * 모든 수정 및 읽기 전용 이벤트 기록 * — 정보를 읽거나 다운로드하는 사용자 작업을 포함한 모든 이벤트를 표시합니다. |

5. 저장 * 을 클릭합니다.

감사 로그에서 이벤트를 삭제합니다

이전 이벤트의 감사 로그를 지울 수 있으므로 이벤트 검색을 보다 쉽게 관리할 수 있습니다. 삭제 시 이전 이벤트를 CSV(쉼표로 구분된 값) 파일에 저장할 수 있습니다.

시작하기 전에

보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. Audit Log(감사 로그) * 탭을 선택합니다.
3. 삭제 * 를 선택합니다.

감사 로그 삭제 대화 상자가 열립니다.

4. 삭제할 가장 오래된 이벤트 수를 선택하거나 입력합니다.
5. 삭제된 이벤트를 CSV 파일로 내보내려면(권장) 확인란을 선택한 상태로 유지합니다. 다음 단계에서 * 삭제 * 를 클릭하면 파일 이름과 위치를 입력하라는 메시지가 표시됩니다. 그렇지 않으면 이벤트를 CSV 파일에 저장하지 않으려면 확인란을 클릭하여 선택을 취소합니다.
6. 삭제 * 를 클릭합니다.

확인 대화 상자가 열립니다.

7. 필드를 입력한 delete 다음 * 삭제 * 를 클릭합니다.

가장 오래된 이벤트는 감사 로그 페이지에서 제거됩니다.

감사 로그를 위해 **syslog** 서버를 구성합니다

감사 로그를 외부 syslog 서버에 보관하려는 경우 해당 서버와 스토리지 시스템 간의 통신을 구성할 수 있습니다. 연결이 설정되면 감사 로그가 syslog 서버에 자동으로 저장됩니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- syslog 서버 주소, 프로토콜 및 포트 번호를 사용할 수 있어야 합니다. 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
- 서버에서 보안 프로토콜(예: TLS)을 사용하는 경우 로컬 시스템에서 인증 기관(CA) 인증서를 사용할 수 있어야 합니다. CA 인증서는 서버와 클라이언트 간의 보안 연결을 위해 웹 사이트 소유자를 식별합니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 감사 로그 탭에서 * Syslog 서버 구성 * 을 선택합니다.

Configure Syslog Servers 대화 상자가 열립니다.

3. 추가 * 를 클릭합니다.

Add Syslog Server 대화 상자가 열립니다.

4. 서버에 대한 정보를 입력한 다음 * 추가 * 를 클릭합니다.
 - * 서버 주소 * — 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
 - * 프로토콜 * — 드롭다운 목록에서 프로토콜을 선택합니다(예: TLS, UDP 또는 TCP).
 - * 인증서 업로드(선택 사항) * — TLS 프로토콜을 선택했지만 아직 서명된 CA 인증서를 업로드하지 않은 경우 * 찾아보기 * 를 클릭하여 인증서 파일을 업로드합니다. 감사 로그는 신뢰할 수 있는 인증서가 없는 syslog 서버에 보관되지 않습니다.



나중에 인증서가 유효하지 않게 되면 TLS 핸드셰이크가 실패합니다. 따라서 오류 메시지가 감사 로그에 게시되고 메시지가 더 이상 syslog 서버로 전송되지 않습니다. 이 문제를 해결하려면 syslog 서버의 인증서를 수정한 다음 설정 [감사 로그 > Syslog 서버 구성 > 모두 테스트] 메뉴로 이동해야 합니다.

- * Port * — syslog 수신기의 포트 번호를 입력합니다. Add * 를 클릭하면 Configure Syslog Servers 대화 상자가 열리고 구성된 syslog 서버가 페이지에 표시됩니다.

5. 스토리지 배열과의 서버 연결을 테스트하려면 * Test All * 을 선택합니다.

결과

구성 후 모든 새 감사 로그가 syslog 서버로 전송됩니다. 이전 로그는 전송되지 않습니다. 경고에 대한 syslog 설정을 추가로 구성하려면 를 참조하십시오 ["경고에 대한 syslog 서버를 구성합니다"](#).

NOTE: If multiple syslog servers are configured, all configured syslog servers will receive an audit log.

감사 로그 레코드에 대한 **syslog** 서버 설정을 편집합니다

감사 로그 아카이빙에 사용되는 syslog 서버의 설정을 변경하고 서버에 대한 새 CA(인증 기관) 인증서를 업로드할 수도 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- syslog 서버 주소, 프로토콜 및 포트 번호를 사용할 수 있어야 합니다. 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
- 새 CA 인증서를 업로드하는 경우 로컬 시스템에서 인증서를 사용할 수 있어야 합니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 감사 로그 탭에서 * Syslog 서버 구성 * 을 선택합니다.

구성된 syslog 서버가 페이지에 표시됩니다.

3. 서버 정보를 편집하려면 서버 이름 오른쪽에 있는 * Edit * (연필) 아이콘을 선택한 후 다음 필드에서 원하는 대로 변경합니다.
 - * 서버 주소 * — 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
 - * 프로토콜 * — 드롭다운 목록에서 프로토콜을 선택합니다(예: TLS, UDP 또는 TCP).
 - * Port * — syslog 수신기의 포트 번호를 입력합니다.
4. 프로토콜을 보안 TLS 프로토콜(UDP 또는 TCP)으로 변경한 경우 * 신뢰할 수 있는 인증서 가져오기 * 를 클릭하여 CA 인증서를 업로드합니다.
5. 스토리지 배열과의 새 연결을 테스트하려면 * Test All * 을 선택합니다.

결과

구성 후 모든 새 감사 로그가 syslog 서버로 전송됩니다. 이전 로그는 전송되지 않습니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.